FINITE PROJECTIVE PLANE GEOMETRIES AND DIFFERENCE SETS

BY

GERALD BERMAN

1. **Introduction.** A set of integers d_j $(j=0, 1, \cdots, m)$ is called a *difference set* $\{d_j\}$ mod $q=m^2+m+1$ if among the differences d_i-d_j mod q $(i, j=0, 1, \cdots, m; i\neq j)$ each of the residues $1, 2, \cdots, q-1$ occurs eactly once. Singer [7] showed the existence of such a set if m is of the form p^n where p is a prime. A difference set is called *reduced* if $d_0=0$, $d_1=1$ and each of the integers is in the range $1, 2, \cdots, q-1$. Any difference set may be reduced by the addition of an integer and reduction mod q. Two difference sets whose corresponding reduced difference sets contain the same integers are called *equivalent.*

If t is an integer relatively prime to q, the set of integers $\{td_j\}$ is a difference set whenever $\{d_j\}$ is a difference set. In the case $m=p^n$ Singer conjectured: (i) The difference set $\{td_j\}$, where t is relatively prime to q, is equivalent to the difference set $\{d_j\}$ if and only if t is a power of p mod q. (ii) If $\{d_j\}$ and $\{d_j'\}$ are any two difference sets containing the same number of elements, there exists an integer t for which $\{td_j\}$ is equivalent to $\{d_j'\}$. It is not yet known whether difference sets exist for which m is not a power of a prime [1].

In this paper difference sets which correspond to finite Desarguesian geometries are studied with the aid of Galois fields. Simple constructions are given for these difference sets, and the two conjectures of Singer are proved for them. It is conjectured that all possible difference sets are of this type.

2. **Two representations for the points of $S\equiv PG(2, p^n)$.** Let S be a finite projective plane having $m+1$ points on each line. It may easily be shown that S contains exactly q points. The following two theorems, first proved by Singer, show the intimate connection between difference sets and finite projective planes.

THEOREM 2.1. *If S admits a collineation ϕ which cyclically permutes the q points, a difference set may be derived as follows. Let the points be named P_i $(i=0, 1, \cdots, q-1)$ in such a way that $P_i=\phi^iP_0$; then if P_{d_j} $(j=0, 1, \cdots, m)$ are the points of a line, $\{d_j\}$ is a difference set* mod q. *The choice of different lines leads to equivalent difference sets.*

THEOREM 2.2. *If $\{d_j\}$ is a difference set* mod q, *and if lines L_i $(i=0, 1, \cdots, q-1)$ of S are defined to be the sets of points d_j+i $(j=0, 1, \cdots, m)$ where the*

Presented to the Society, April 25, 1952; received by the editors May 10, 1952 and, in revised form, August 1, 1952.

points of S are the residue classes of integers mod q, *then S is a projective plane.*

The proofs of these theorems do not require the assumption of Desargues' theorem. However, no such collineation ϕ has been discovered in a non-Desarguesian plane, and every known difference set yields a Desarguesian plane. For the remainder of the paper we shall assume that $m=p^n$ and consider the finite Desarguesian plane S having $m+1$ points on each line. S is uniquely defined by the integer m and is usually denoted by $PG(2, m)$. In this case it has been shown that there exists a collineation ϕ, transitive on both the points and lines of S [6, 7, 8]. It follows by Theorem 2.1 that there exists a unique reduced difference set corresponding to $PG(2, m)$ for every $m=p^n$.

The points of S may also be represented by elements of the Galois field $K\equiv GF(p^{3n})$. A point is defined to be the set of elements of K linearly dependent with respect to $F\equiv GF(p^n)\subset K$ on one element of K, and a line to be the set of elements of K linearly dependent with respect to K on two linearly independent elements of K. It is well known that the system so defined is isomorphic to S. We shall identify S with its representations.

To study the connection between these two representations of S, it is convenient to define a subset $E\subset K$ as follows. An element $\alpha\in K$ belongs to the subset E if $\alpha^q\in F$ and $\alpha^i\notin F$ for any i $(0<i<q)$. E contains $(m-1)\phi(q)$ elements (where ϕ is Euler's ϕ-function). The set of primitive elements Λ of K belongs to E. It can be shown that $E=\Lambda$ if and only if $p^n=2$ or $p^n=4$. Since every element of E satisfies an irreducible cubic F-equation, every power α^i $(i=0, 1, \cdots, q-1)$ of any element $\alpha\in E$ may be expressed in the form $\alpha^i=a_i+b_i\alpha+c_i\alpha^2\equiv f_i(\alpha)$, where a_i, b_i, c_i are elements of F. In particular, if $\alpha\in\Lambda$, any three elements of F not all zero uniquely determine a power of α and hence a nonzero element of K. The letter λ will be used to denote a primitive element. We now prove three lemmas.

LEMMA 2.1. *$\alpha^c\in F$ for any $\alpha\in E$ if and only if $c\equiv 0$* mod q.

LEMMA 2.2. *Every nonzero element of K which belongs to F may be expressed uniquely in the form λ^{iq} $(0\leqq i\leqq m-2)$ where λ is any element of Λ.*

LEMMA 2.3. *Every element of E may be expressed uniquely in the form λ^c $(0<c\leqq q-1)$ with $(c, q)=1$ where λ is any element of Λ.*

Since $\alpha\in E$, $\alpha^{iq}\in F$ for all values of i. Suppose for some c, $\alpha^c\in F$ with $c=aq+b$, $0<b<q$. Then $\alpha^{aq+b}=\alpha^{aq}\alpha^b\in F$ implies that $\alpha^b\in F$, which is impossible. Lemma 2.2 follows from Lemma 2.1 and the fact that λ is a primitive element of K. To prove Lemma 2.3, suppose $(c, q)=d$. Then $c=dc'$, $q=dq'$ with $(c', q')=1$, and $(\lambda^c)^{q'}=(\lambda^{dq'})^{c'}\in F$. By definition, $\lambda^c\in F$ if and only if $q'=q$ so that $d=1$. The expression is unique since λ is primitive. It follows at once that the number of elements of E is $(m-1)\phi(q)$.

THEOREM 2.3. *The points of S may be represented in the form α^i $(i=0, 1, \cdots, q-1)$, where α is any element of E.*

It is sufficient to show that no two of the elements α^i $(i=0, 1, \cdots, q-1)$ are linearly dependent with respect to F. Suppose $\alpha^k=a\alpha^j$ for some $j<k<q$ and some $a\in F$. Then $\alpha^{k-j}=a\in F$ with $k-j<q$. This is impossible by Lemma 2.1. If we write i for α^i $(i=0, 1, \cdots, q-1)$, we have

THEOREM 2.3′. *The points of S may be represented by the integers $0, 1, \cdots, q-1$. Three points r, s, t are collinear if and only if there exist elements $a, b, c\in F$ such that $a\alpha^r+b\alpha^s+c\alpha^t=0$.*

THEOREM 2.4. *Two elements α^r, α^s of K where $\alpha\in E$ represent the same point of S if and only if $r\equiv s \pmod q$.*

If $r\equiv s \pmod q$, there exists an integer t such that $r=s+tq$, so that $\alpha^r=a\alpha^s$, where $a=\alpha^{tq}$ by Lemma 2.1. On the other hand, if α^r and α^s represent the same point, there exists an element $a\in F$ such that $\alpha^r=a\alpha^s$. Let λ be any element of Λ. By Lemma 2.2, $a=\lambda^{tq}$ for some t, and by Lemma 2.3, $\alpha=\lambda^c$ for some c relatively prime to q. Then $\lambda^{cr}=\lambda^{tq+cs}$, so that $cr\equiv cs \pmod q$. Since $(c, q)=1$, $r\equiv s \pmod q$. Corresponding to Theorem 2.3′ we have

THEOREM 2.4′. *Two integers r, s represent the same point of S if and only if $r\equiv s \pmod q$.*

THEOREM 2.5. *Multiplication of the elements of K by α is a collineation in S.*

This follows since $a\alpha^r+b\alpha^s+c\alpha^t=0$ implies that $a\alpha^{r+1}+b\alpha^{s+1}+c\alpha^{t+1}=0$.

THEOREM 2.5′. *Addition of an integer modulo q is a collineation in the integer representation of S.*

Theorems 2.3′, 2.4′, 2.5′ show that the points of S may be represented by residue classes of integers modulo q. The actual integers which represent any particular point depend of course on the choice of $\alpha\in E$. This representation is closely connected with Theorem 2.2. If we set up the correspondence $\alpha^i\rightarrow\phi^iP_0$, the cyclic collineation ϕ corresponds to the multiplication of the points of S by α. In the integer representation the collineations ϕ and α both correspond to the addition of an integer modulo q. It is clear that α dedetermines the collineation ϕ uniquely and hence determines a class of equivalent difference sets by Theorem 2.1. The set of all difference sets determined in this way for all choices of $\alpha\in E$ will be denoted by $\mathfrak{D}$. A maximal subset of inequivalent difference sets will be denoted by $\mathfrak{D}'$.

3. **The relationship between $\mathfrak{D}$ and E.** It was pointed out that every power α^i $(i=0, 1, \cdots, q-1)$ of an element $\alpha\in E$ can be expressed in the form $\alpha^i=a_i+b_i\alpha+c_i\alpha^2\equiv f_i(\alpha)$. This leads to a simple construction for difference sets.

THEOREM 3.1. *Let $f_{d_j}(\alpha)$ $(j=0, 1, \cdots, m)$ be the subset of the polynomials $f_i(\alpha)$ $(i=0, 1, \cdots, q-1)$ having degree less than two. Then $\{d_j\}$ is a difference set in reduced form.*

Each of the polynomials $f_{d_j}(\alpha)$ $(j=0, 1, \cdots, m)$ is linearly dependent with respect to F on the elements $1, \alpha$. The corresponding points, being all different by Theorem 2.3, represent all the points on the line of S joining the points $1, \alpha$. By Theorem 2.1, $\{d_j\}$ is a difference set. It is in reduced form since $0 \leqq d_j < q$ $(j=0, 1, \cdots, m)$ and $d_0=0$, $d_1=1$. The difference sets corresponding to the other lines of S are of the form $\{d_j+i\}$ $(i=0, 1, \cdots, q-1)$. All the difference sets of $\mathfrak{D}$ can be constructed in this way. They are not all equivalent, however.

We shall say that a difference set corresponds to an element $\alpha \in E$ if it can be obtained from α by Theorem 3.1.

THEOREM 3.2. *Two elements $\alpha=\lambda^r, \beta=\lambda^s, \lambda \in \Lambda$, $(r, q)=(s, q)=1$, correspond to equivalent difference sets if $r \equiv s \pmod{q}$.*

Let $s=kq+r$, so that $\lambda^s=a\lambda^r$ where $a=\lambda^{kq} \in F$. Let $\{d_j\}$ be the difference set corresponding to α. By Theorem 3.1, $\alpha^{d_j}=a_j+b_j\alpha$ $(a_j, b_j \in F)$ for all $j=0, 1, \cdots, m$. But $\alpha=a^{-1}\beta$, so that $\beta^{d_j}=a_j'+b_j'\beta$ where $a_j'=a_j a^{d_j-1} \in F$ and $b_j'=b_j a^{d_j-1} \in F$. Since no two expressions for β^{d_j} are linearly dependent, $\{d_j\}$ is the difference set corresponding to β.

COROLLARY 3.21. *α, β correspond to equivalent difference sets if there exists an $a \in F$ such that $\beta=a\alpha$.*

Theorem 3.2 shows that all the inequivalent difference sets of S are contained among the difference sets corresponding to the $\phi(q)$ elements of E of the form α^i, $(i, q)=1$ $(0<i<q)$, where α is an element of Λ. We now show that there $\phi(q)$ elements group themselves into sets of $3n$ elements which correspond to equivalent difference sets.

THEOREM 3.3. *The elements α^{p^i} $(\alpha \in E;\ i=0, 1, \cdots, 3n-1)$ correspond to equivalent difference sets.*

The correspondence $x \to x^{p^i}$ is an automorphism of K for all $i=0, 1, \cdots, 3n-1$ [9], and induces a collineation in S. The collinear points α^{d_j} $(j=0, 1, \cdots, m)$ are carried into β^{d_j} $(j=0, 1, \cdots, m)$ where $\beta=\alpha^{p^i} \in E$. It follows that the difference set also corresponds to β. The construction in Theorem 3.1 leads to a difference set $\{d_j'\}$ which must be equivalent to $\{d_j\}$ by Theorem 2.1.

Two elements $\alpha, \beta \in E$ thus correspond to the same difference set if there exists an element $a \in F$ and an integer i such that $\beta=a\alpha^{p^i}$. We now divide E into $\mu=\phi(q)/3n$ disjoint subsets E_i $(i=0, 1, \cdots, \mu-1)$. The subset containing α consists of the $3n(m-1)$ elements of E of the form $a\alpha^{p^i}$, $a \in F$. It is easy to verify that this definition is consistent, being independent of the

element used to define the set. The elements of each set correspond to equivalent difference sets of $\mathfrak{D}$. A set of representative elements, one chosen from each set E_i $(i=0, 1, \cdots, \mu-1)$ will be denoted by E'. Before showing that the elements of E' correspond to inequivalent difference sets, we prove

LEMMA 3.1. *The elements of E' may be selected from Λ.*

It is sufficient to show that among the elements $\beta=a\alpha^{p^i}$ $(a\in F, \alpha\in E, 0\leqq i<3n-1)$ there is at least one primitive element. If α is not primitive, choose any primitive element λ. Then $\alpha=\lambda^r$, $(r, q)=1$; and $\beta=\lambda^t$, where $a=\lambda^{sq}$ and $t=rp^i+sq$. Consider the arithmetic sequence $t_s=rp^i+sq$ $(s=0, 1, \cdots)$. An infinite number of these are primes [6]. Thus we can choose $t=t_\sigma$ a prime greater than $p^{3n}-1$. Then $(t_\sigma, p^{3n}-1)=1$. Write t_σ in the form $t_\sigma=u(p^{3n}-1)+v$. This can always be done so that $0<v<p^{3n}-1$. The element λ^{t_σ} of K is a primitive element, for $\lambda^{t_\sigma}=\lambda^v$ with $(v, p^{3n}-1)=1$.

Since the above argument is independent of i, we have actually shown that each set E_i contains $3n$ primitive elements. It will usually be convenient to choose the representative elements E' to be primitive.

THEOREM 3.4. *There is a 1-1 correspondence between the difference sets of $\mathfrak{D}'$ and the elements of E'.*

Let α, β be two elements of E, such that α is primitive and $\beta=\alpha^k$ with $(k, q)=1$, $1<k<q$. (Elements of both these types belong to every set E_i.) In the representation α the points on one of the lines of S is expressible in the form $\alpha^d=a+b\alpha$ where a, b range over F and d ranges over the difference set $\{d_j\}$. Taking the kth power of each of these expressions, we obtain $\alpha^{dk}=\beta^d=(a+b\alpha)^k$. If $\{d_j\}$ is also the difference set corresponding to β, then these expressions must represent the points of a line of S in the representation β. This must be the line joining 1, β, since a, b take any values in F. Thus the expressions $(a+b\alpha)^k$ must be linearly dependent on 1, β. Let $\alpha^i=r_j+s_j\beta+t_j\beta^2$ $(j=0, 1, \cdots, k-1)$. Then

$$(a+b\alpha)^k = a^k + b^k\beta + \sum_{j=1}^{k-1}\binom{k}{j} a^{k-i}b^i(r_j + s_j\beta + t_j\beta^2).$$

If $k\neq 0$ in F, the coefficient of β^2 must vanish for all choices of a, b in F. If $k\neq 2$, we have $t_1=t_2=0$, so that 1, α, α^2 are collinear, which is impossible. If $k=2$ we have $t_1=0$, $\alpha^2=\beta=s_1^{-1}(\alpha-r_1)$, and 1, α, α^2 are again collinear. Hence $k=0$ considered as an element of F; that is, k must be of the form p^i. This means that α, β correspond to the same difference set if and only if they are in the same set E_i. Theorems 4.1 and 4.2 are immediate corollaries. Since there are $\phi(q)/3n$ elements in E', we also have

COROLLARY 3.41. *There are exactly $\phi(q)/3n$ inequivalent difference sets* mod q.

To make the present discussion complete, we shall now show how the elements of E corresponding to a given reduced difference set $\{d_j\}$ may be constructed. Let x be an element of E which corresponds to the difference set. There exist integers r, s such that $d_s - d_r = 2$. Let $x^{d_r} = a + bx$, $x^{d_s} = c + dx$, where a, b, c, d are elements of F to be determined. Then $x^{d_r+2} = x^{d_s}$ so that $x^3 = b^{-1}(c + dx - ax^2)$. Multiply both sides of this expression successively by x and each time replace x^3 by its expression in terms of a, b, c, d. This yields expressions for x^i $(i = 4, 5, \cdots)$ in terms of a, b, c, d. In particular, we must have $x^{d_r} = a + bx$. The corresponding identity yields three equations for the four unknowns. These equations have solutions in F, since the elements of E corresponding to the difference set exist. There will be $n(m-1)$ solutions, each leading to an irreducible cubic whose roots are elements of E corresponding to the difference set. All the cubics may be deduced from any one of them; for if α is an element of E corresponding to a difference set, the other elements of E corresponding to equivalent difference sets may be written in the form $\beta = a\alpha^{p^i}$ $(a \in F)$. If β satisfies the equation $f(x) = 0$, then α will satisfy the equation $f(ax^{p^i}) = 0$.

THEOREM 3.5. *Every difference set corresponds to a set of $n(m-1)$ cubic F-polynomials whose roots in K are the elements of E corresponding to the difference set. If $f(x)$ is any one of these polynomials, any one of the others may be expressed in the form $f(ax^{p^i})$ $(a \in F,\ 0 \leqq i < 3n-1)$.*

Theorem 3.5 shows that it is necessary to find only one set of solutions (a, b, c, d) in the previous construction to obtain all $n(m-1)$ F-polynomials, and hence all $3n(m-1)$ elements of E corresponding to a given difference set.

4. Difference sets and multipliers. All the difference sets of $\mathfrak{D}$ can be constructed by Theorem 3.1 when the elements of the set E' are known. In this section we shall show how they may be derived from any one of them, so that it is only necessary to apply Theorem 3.1 to one element of E.

An integer t will be called a *multiplier* of the difference set $\{d_j\}$ if $\{td_j\}$ is a difference set. (This differs from the definition used by Marshall Hall, Jr. [6]. He called t a multiplier if the difference sets $\{d_j\}$ and $\{td_j\}$ were equivalent.) It is clear that t may always be taken less than q, since the difference sets are taken mod q.

THEOREM 4.1. *t is a multiplier of the difference set $\{d_j\}$ if and only if $(t, q) = 1$.*

Let the difference set correspond to the primitive element λ. Let t be any integer such that $(t, q) = 1$. Then there exists a primitive element μ and an integer r such that $\lambda = \mu^{t+rq} = a\mu^t$ where $a = \mu^{rq} \in F$. But $\lambda^{d_j} = a_j + b_j\lambda$ $(a_j, b_j \in F;\ j = 0, 1, \cdots, m)$, so that $\mu^{td_j} = a_j' + b_j'\mu^t$ $(j = 0, 1, \cdots, m)$ where $a_j', b_j' \in F$. The $m+1$ points μ^{td_j} $(j = 0, 1, \cdots, m)$, being linearly dependent on 1, μ^t, are on the line joining 1, μ^t. They are distinct, for if we had $\mu^{td_j} = \mu^{td_k}$, then

μ^t would not belong to E unless $j=k$. By Theorem 2.1, $\{td_j\}$ is a difference set. If $(t, q)\neq 1$, μ^t would not belong to E and so could not correspond to a difference set.

Since the condition $(t, q)=1$ is independent of the difference set $\{d_j\}$, we have

COROLLARY 4.11. *If t is a multiplier of one difference set* mod q, *then t is a multiplier of every difference set* mod q.

We shall refer to t as a multiplier of S.

COROLLARY 4.12. *There are exactly $\phi(q)$ multipliers of S.*

An alternative proof of Theorem 4.1 can easily be given by going back to the original definition of a difference set.

THEOREM 4.2. *The difference sets $\{d_j\}$ and $\{td_j\}$ are equivalent if and only if t is of the form p^k* mod q.

Two elements λ, λ' of Λ correspond to the same difference set if and only if there exists an element $a\in F$ and an integer k such that $\lambda'=a\lambda^{p^k}$. Taking $t=p^k$ in the proof of Theorem 4.1 yields the required result.

Since $(t, q)=1$, $(t', q)=1$ implies that $(tt', q)=1$, the product of two multipliers is a multiplier. In particular tp^i is a multiplier whenever t is a multiplier. By Theorem 4.2 if t, t' are multipliers and $\{d_j\}$ is any difference set, then the difference sets $\{td_j\}$ and $\{t'td_j\}$ are equivalent if and only if t' is of the form p^i mod q. Two multipliers which carry a difference set into equivalent difference sets will be called equivalent multipliers. Thus we have

THEOREM 4.3. *Two multipliers t_1, t_2 are equivalent if and only if there exists an integer k such that $t_2\equiv p^k t_1$* (mod q).

It is clear that the $\phi(q)$ multipliers form a group under multiplication mod q, and divide themselves into sets of $3n$ equivalent multipliers.

THEOREM 4.4. *The multipliers of S form an abelian group G of order $\phi(q)$. The multipliers of the form p^i* (mod q) *form a cyclic subgroup H of order $3n$. H divides G into $\mu=\phi(q)/3n$ cosets of equivalent multipliers.*

A set of μ inequivalent multipliers will be called *complete*. Since each multiplier of a complete set of multipliers yields a different difference set, no two of which are equivalent, and since there are exactly μ inequivalent difference sets (Corollary 3.4) we have

THEOREM 4.5. *Let t_i $(i=1, 2, \cdots, \mu)$ be a complete set of multipliers of S. Let $\{d_j\}$ be any difference set. Then $\{t_i d_j\}$ $(i=1, 2, \cdots, \mu)$ is a complete set of inequivalent difference sets.*

Since the addition of an integer s to the elements of a difference set yields an equivalent difference set, and since all equivalent difference sets may be obtained in this way, we have

THEOREM 4.6. *Every difference set* mod q *is of the form* $\{d_j'\}$ *where* $d_j' = s + td_j$, $(t, q) = 1$, *and* $\{d_j\}$ *is any difference set* mod q.

COROLLARY 4.61. *Let* $\{d_j\}$ *and* $\{d_j'\}$ *be any two difference sets* mod q, *then there exist integers* s, t *such that the residues* $s + td_j$ (mod q) *are a rearrangement of the* d_j' (mod q).

This may be stated in a slightly different form:

COROLLARY 4.62. *If* $\{d_j\}$ *and* $\{d_j'\}$ *are any two difference sets* mod q, *then there exists an integer* t *such that* $\{td_j\}$ *is equivalent to* $\{d_j'\}$.

REFERENCES

1. R. H. Bruck and H. J. Ryser, *The nonexistence of certain finite projective planes*, Canadian Journal of Mathematics vol. 1 (1949) pp. 88–94.

2. W. H. Bussey, *Tables of Galois fields*, Bull. Amer. Math. Soc. vol. 12 (1905–06) pp. 22–38.

3. ———, *Tables of Galois fields*, Bull. Amer. Math. Soc. vol. 16 (1909–10) pp. 188–206.

4. R. D. Carmichael, *Introduction to the theory of groups of finite order*, Boston, 1937.

5. Marshall Hall, Jr., *Cyclic projective planes*, Duke Math. J. vol. 14 (1947) pp. 1079–1090.

6. A. Selberg, *An elementary proof of Dirichlet's theorem about primes in an arithmetic progression*, Ann. of Math. vol. 50 (1949) pp. 297–304.

7. James Singer, *A theorem of finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. vol. 43 (1938) pp. 377–385.

8. E. Snapper, *Periodic linear transformations of affine and projective geometries*, Canadian Journal of Mathematics vol. 2 (1950) pp. 149–151.

9. B. L. van der Waerden, *Moderne algebra*, Berlin, 1937.

ILLINOIS INSTITUTE OF TECHNOLOGY,
CHICAGO, ILL.